Claims

1. A management apparatus that manages a plurality of terminal apparatuses by arranging apparatus identifiers for identifying the plurality of terminal apparatuses to be leaves of a tree structure and assigning pieces of unique information to the apparatus identifiers respectively, the pieces of unique information being bases of decryption keys for decrypting a piece of encrypted data, the management apparatus comprising:

a subset generating unit operable to calculate and generate, for each of nodes in layers except for the leaves of the tree structure, a subset being made up of one or more apparatus identifiers positioned subordinate to the node;

a first association unit operable to search for a subset that wholly contains another subset positioned in a lowermost layer other than a leaf layer from an immediately upper layer, and to associate the subsets with each other;

a second association unit operable to search for another subset that wholly contains the containing subset being an association destination from a same layer or an immediately upper layer and to associate the subsets with each other;

a first control unit operable to control the second association unit so that processing thereof is repeatedly performed up to an uppermost layer;

a second control unit operable to control the first association unit, the second association unit, and the first control unit so that processings thereof are repeatedly performed on all subsets in the lowermost layer;

a first assignment unit operable to bring pieces of unique information into correspondence with the subsets in the lowermost layer respectively and to assign each piece of unique information to apparatus identifiers contained in the corresponding subset in the lowermost layer; and

a second assignment unit operable to bring pieces of derivative unique information into correspondence respectively with subsets each of which extends over two or more layers as a result of the associating and to assign each piece of derivative unique information to apparatus identifiers contained in the corresponding extending subset, the pieces of derivative unique information being derivatively obtained from the pieces of unique information.

2. The management apparatus of Claim 1, wherein

the subset that is searched for by the first association unit and wholly contains said another subset in the lowermost layer is made up of a smallest number of elements, and the first association unit associates said another subset being a parent node with the searched subset being a child node,

the subset that is searched for by the second association unit and wholly contains the containing subset being the association destination is made up of a smallest number of elements, and the second association unit associates the association destination subset being a parent node with the searched subset being a child node, and

the first control unit controls the second association unit so that processing thereof is performed repeatedly up to the uppermost layer and generates subset trees whose roots are the subsets in the

lowermost layer.

3. The management apparatus of Claim 2, wherein

the first association unit controls the second association unit so that processings thereof are repeatedly performed up to the uppermost layer, using one or more subsets obtained by excluding one or more subsets having been associated from subsets positioned in upper layers of the lowermost layer and generates subset trees whose roots are the subsets in the lowermost layer.

4. The management apparatus of Claim 3, wherein

the second assignment unit generates the pieces of derivative unique information from the pieces of unique information, using a one-way function and brings the generated pieces of derivative unique information into correspondence with the extending subsets.

5. The management apparatus of Claim 4, further comprising:

a unique information obtaining unit operable to obtain, in a case where a subset in which an identifier of a terminal apparatus being a distribution destination of a piece of unique information appears as an element for a first time exists on one or more paths from the roots to one or more leaves of the subset trees, one or more pieces of unique information being in correspondence with such a subset; and

a distributing unit operable to distribute, to the terminal apparatus being the distribution destination, one or more groups each being made up of a different one of the obtained pieces of unique information and set identification information that identifies the

subset that is in correspondence with the piece of unique information.

6. The management apparatus of Claim 5, wherein

the unique information obtaining unit includes:

a first obtaining unit operable to search for the subset in which the identifier of the terminal apparatus being the distribution destination appears as an element for the first time in the one or more paths from the roots to the one or more leaves of the subset trees and, in the case where such a subset has been detected and has not been obtained, to obtain the detected subset;

a second obtaining unit operable to obtain the one or more pieces of unique information that are in correspondence with the subset obtained by the first obtaining unit; and

a repetition controlling unit operable to control the first and second obtaining units so that processings thereof are repeatedly performed until all of the one or more paths are searched.

7. The management apparatus of Claim 5, further comprising:

a first storing unit having an area for storing subsets being constituent elements of the subset trees and pieces of unique information that are respectively in correspondence with the subsets;

a second storing unit having an area for storing a plurality of nodes constituting the subset trees and child nodes of the plurality of nodes;

a first writing unit operable to write the subsets and the pieces of unique information into the first storing unit, while the subsets are brought into correspondence with the pieces unique information; and

a second writing unit operable to write the plurality of nodes and the child nodes of the plurality of nodes into the second storing unit, while the nodes are brought into correspondence with the child nodes.

8. The management apparatus of Claim 7, wherein

the first storing unit has a first table storing therein a plurality of groups each being made up of a different one of the subsets and the corresponding piece of unique information,

the second storing unit has a second table storing therein a plurality of groups each being made up of a different one of the nodes and the corresponding child node,

the first writing unit writes the groups made up of the subsets and the corresponding pieces of unique information into the first table, and

the second writing unit writes the groups made up of the nodes and the child nodes into the second storing unit.

9. The management apparatus of Claim 7, wherein

the second control unit generates a plurality of subset trees by controlling the first association unit, the second association unit, and the first control unit so that the processings thereof are repeatedly performed on all the subsets in the lowermost layer,

the first storing unit stores therein subsets contained in the plurality of subset trees and pieces of unique information that are in correspondence with the contained subsets, and

the management apparatus further comprises:

a revoked identifier storing unit having an area for

storing one or more revoked identifiers indicating one or more revoked terminal apparatuses out of the plurality of terminal apparatuses;

an encryption key generating unit operable to obtain one or more of the subsets from the first storing unit based on what is stored in the revoked identifier storing unit, to obtain one or more encryption keys based on pieces of unique information that are respectively in correspondence with the obtained subsets, to encrypt a media key used for utilization of a content with the obtained encryption keys individually, so as to generate encrypted media keys that are equal in number to the one or more encryption keys; and

a third writing unit operable to write, onto a recording medium mounted on the management apparatus, one or more groups each being made up of a different one of the encrypted media keys and a piece of reference identification information for identifying a subset used for obtaining the encryption key for the encrypted media key.

10. The management apparatus of Claim 9, further comprising:

a revoked identifier receiving unit operable to receive each revoked identifier and write the received revoked identifier into the revoked identifier storing unit.

11. The management apparatus of Claim 9, wherein

the encryption keys are each a common key and are identical to the decryption keys,

the one-way function is further used for generating common keys based on the pieces of unique information from the pieces of unique information, and

the encryption key generating unit includes:

a subset obtaining unit operable to obtain, from the first storing unit, a subset that contains a largest number of one or more unrevoked identifiers which are other than the revoked identifiers stored in the revoked identifier storing unit;

a control unit operable to control the subset obtaining unit so that processing thereof is repeatedly performed until each of all the unrevoked identifiers belongs to any one of the one or more subsets obtained by the subset obtaining unit;

a common key obtaining unit operable to obtain, using the one-way function, one or more common keys generated from the pieces of unique information that are respectively in correspondence with the subsets obtained by the subset obtaining unit; and

an encrypting unit operable to generate encrypted media keys that are equal in number to the common keys, using the common keys obtained by the common key obtaining unit.

12. The management apparatus of Claim 9, wherein

each piece of reference identification information is a corresponding subset used for obtaining a corresponding common key for the encrypted media key,

the third writing unit writes, onto the recording medium, one or more groups each being made up of a different one of the encrypted media keys and the corresponding subset used for obtaining the corresponding common key for the encrypted media key,

the distributing unit distributes, to the terminal apparatus being the distribution destination, one or more groups each being made up of a different one of the obtained pieces of unique information

and a piece of set identification information that is one of the subsets with which the piece of unique information is in correspondence, and

the distributing unit further distributes a data structure indicating the subset trees.

13. The management apparatus of Claim 9, further comprising:

a path information obtaining unit operable to obtain a piece of path information including (i) a generation path indicating, for each subset, a path that extends from a root subset being a root of a subset tree to which the subset belongs and reaches the subset, and (ii) a root identifier indicating the root subset, wherein

the reference identification information is a piece of path information for the subset used for obtaining the encryption key for the encrypted media key,

the third writing unit writes, onto the recording medium, one or more groups each being made up of a different one of the encrypted media keys and a piece of path information for the subset used for obtaining the encryption key for the encrypted media key, and

the distributing unit distributes, to the terminal apparatus being the distribution destination, one or more groups each being made up of a different one of the obtained pieces of unique information and a piece of set identification information that is a piece of path information for the subset with which the obtained piece of unique information is in correspondence.

14. A terminal apparatus to which a piece of unique information being a base of a decryption key for decrypting a piece of encrypted

data is assigned by a management apparatus that manages, with use of a tree structure, a plurality of apparatus identifiers identifying a plurality of terminal apparatuses, wherein

the management apparatus (i) calculates and generates, for each of nodes in layers except for leaves of the tree structure, a subset being made up of one or more apparatus identifiers positioned subordinate to the node, (ii) searches for a subset that wholly contains another subset positioned in a lowermost layer other than a leaf layer from an immediately upper layer and associates the subsets with each other, (iii) searches for a subset that wholly contains the containing subset from a same layer or an immediately upper layer and associates the subsets with each other, (iv) controls a second association unit so that the associating is repeatedly performed up to an uppermost layer, (v) performs control so that these processings are repeatedly performed on all subsets in the lowermost layer, (vi) brings pieces of unique information into correspondence with the subsets in the lowermost layer and assigns each piece of unique information to apparatus identifiers contained in the corresponding subset in the lowermost layer, and (vii) brings pieces of derivative unique information into correspondence respectively with subsets each of which extends over two or more layers as a result of the associating and assigns each piece of derivative unique information to apparatus identifiers contained in the corresponding extending subset, the pieces of derivative unique information being derivatively obtained from the pieces of unique information, and

the terminal apparatus includes

a unique information storing unit storing therein a piece of unique information that contains an apparatus identifier of the

terminal apparatus, out of the pieces of unique information that have been distributed from the management apparatus in advance and are brought into correspondence with the subsets.

15. The terminal apparatus of Claim 14, wherein

the unique information storing unit further stores therein a piece of set identification information identifying a subset with which the stored piece of unique information is in correspondence, and

the terminal apparatus further includes:

a judging unit operable to judge whether the piece of set identification information indicates that the terminal apparatus is an unrevoked apparatus;

a first obtaining unit operable to, in a case where a judgment result of the judgment unit is in the affirmative, obtain an encrypted media key that (i) is obtained by encrypting a media key with an encryption key based on a specific piece of unique information out of the pieces of unique information in correspondence with the subsets generated by the management apparatus and (ii) is in correspondence with a piece of key related information related to the encryption key;

a second obtaining unit operable to obtain a decryption key that is in correspondence with the encryption key using the piece of unique information stored in the unique information storing unit; and

a decrypting unit operable to decrypt the encrypted media key obtained by the first obtaining unit, using the decryption key obtained by the second obtaining unit, so as to generate the

media key.

16. The terminal apparatus of Claim 15, wherein

the specific piece of unique information is a piece of reference unique information that is in correspondence with a subset that contains, at a time when the encrypted media key is generated, one or more identifiers of one or more unrevoked apparatuses,

the encryption key is a common key,

the piece of key related information is a piece of reference identification information that identifies the subset with which the piece of reference unique information is in correspondence,

the encrypted media key is in correspondence with the piece of reference identification information,

the judgment unit judges that the piece of set identification information indicates that the terminal apparatus is an unrevoked apparatus, in a case where a path exists that extends from the subset identified by the piece of set identification information stored in the unique information storing unit and reaches the subset identified by the piece of reference identification information,

the first obtaining unit obtains the encrypted media key that is encrypted by an encryption key based on the piece of reference unique information in correspondence with the piece of reference identification information,

the second obtaining unit obtains the decryption key and takes the obtained decryption key as the common key, and

the decrypting unit decrypts the encrypted media key, using the obtained common key.

17. The terminal apparatus of Claim 16, wherein

the management apparatus (i) searches for a subset that wholly contains said another subset in the lowermost layer and is made up of a smallest number of elements and associates said another subset being a parent node with the searched subset being a child node, (ii) further searches for a subset that wholly contains the containing subset being an association destination, is made up of a smallest number of elements, and has not been associated yet, and associates the association destination subset being a parent node with the further searched subset being a child node, so as to generate subset trees whose roots are the subsets in the lowermost layer,

the unique information storing unit further stores therein a data structure for constituting the subset trees generated by the management apparatus, and

the judgment unit judges, using the subset trees constituted with the data structure, whether or not a path exists that extends from the subset that is in correspondence with the piece of unique information stored in the unique information storing unit and reaches the subset identified by the piece of reference identification information.

18. The terminal apparatus of Claim 16, wherein

the management apparatus (i) searches for a subset that wholly contains said another subset in the lowermost layer and is made up of a smallest number of elements and associates said another subset being a parent node with the searched subset being a child node, (ii) further searches for a subset that wholly contains the containing subset being an association destination, is made up of a smallest

number of elements, and has not been associated yet, and associates the association destination subset being a parent node with the further searched subset being a child node, so as to generate subset trees whose roots are the subsets in the lowermost layer,

the piece of reference identification information includes a first generation path that extends from a root of one of the subset trees and reaches a reference subset with which the piece of reference unique information is in correspondence,

the piece of set identification information includes a second generation path that extends from the root of the one of the subset trees and reaches a subset with which the piece of unique information is in correspondence, and

the judgment unit judges, in a case where the second generation path is contained in the first generation path, that a path exists that extends from the subset identified by the piece of set identification information and reaches the subset identified by the piece of reference identification information.

19. The terminal apparatus of Claim 16, wherein

the management apparatus (i) inputs a piece of unique information that is in correspondence with a subset to a one-way function so as to generate a common key based on the piece of unique information and generate a piece of derivative unique information deriving from the piece of unique information, (ii) brings the generated piece of derivative unique information into correspondence with a subset that is associated with the subset with which the inputted piece of unique information is in correspondence, and (iii) assigns the generated piece of derivative unique information to apparatus

identifiers included in the associated subset,

the second obtaining unit includes:

a device key obtaining unit operable to generate and obtain a device key based on the piece of unique information and the piece of derivative unique information from the piece of unique information stored in the unique information storing unit, using a function identical to the one-way function;

a repetition unit operable to control the device key obtaining unit so that processing thereof is repeatedly performed using each piece of unique information obtained by the device key obtaining unit as a next input to the identical function, until a device key based on the piece of reference unique information is obtained; and

a decryption key obtaining unit operable to obtain, as the common key, the device key based on the piece of reference unique information obtained by the device key obtaining unit.

20. The terminal apparatus of Claim 19, further comprising:

a content obtaining unit operable to obtain a content;

a content key obtaining unit operable to obtain a content key;

a first encrypting unit operable to encrypt the content key obtained by the content key obtaining unit, using the media key obtained by the decrypting unit so as to generate an encrypted content key;

a second encrypting unit operable to encrypt the content obtained by the content obtaining unit, using the content key obtained by the content key obtaining unit so as to generate an encrypted content; and

a writing unit operable to write the encrypted content key

and the encrypted content into a recording medium.

21. The terminal apparatus of Claim 20, wherein

the writing unit writes the encrypted content key and the encrypted content into the recording medium which is included in an apparatus located in a network, via a communication medium.

22. The terminal apparatus of Claim 19, further comprising:

an encrypted content key obtaining unit operable to obtain an encrypted content key which is obtained by encrypting a content key with the media key;

an encrypted content obtaining unit operable to obtain an encrypted content which is obtained by encrypting a content with the content key;

a first decrypting unit operable to decrypt the encrypted content key obtained by the encrypted content key obtaining unit, using the media key so as to generate the content key;

a second decrypting unit operable to decrypt the encrypted content obtained by the encrypted content obtaining unit, using the content key so as to generate the content; and

a playback unit operable to play back the content generated by the second decrypting unit.

23. The terminal apparatus of Claim 22, wherein

the encrypted content key and the encrypted content are recorded on a recording medium, which is mounted on the terminal apparatus,

the encrypted content key obtaining unit obtains the encrypted content key from the recording medium, and

the encrypted content obtaining unit obtains the content from the recording medium.

24. The terminal apparatus of Claim 22, wherein

the encrypted content obtaining unit obtains the encrypted content key via a communication medium, and

the encrypted content obtaining unit obtains the content via a communication medium.

25. A copyright protection system comprising a plurality of terminal apparatuses and a management apparatus that manages the plurality of terminal apparatuses by arranging apparatus identifiers for identifying the plurality of terminal apparatuses to be leaves of a tree structure and assigning pieces of unique information to be bases of decryption keys for decrypting a piece of encrypted data to the apparatus identifiers respectively, wherein

the management apparatus includes:

a subset generating unit operable to calculate and generate, for each of nodes in layers except for the leaves of the tree structure, a subset being made up of one or more apparatus identifiers positioned subordinate to the node;

a first association unit operable to search for a subset that wholly contains another subset positioned in a lowermost layer other than a leaf layer from an immediately upper layer, and to associate the subsets with each other;

a second association unit operable to search for another subset that wholly contains the containing subset being an association destination from a same layer or an immediately upper layer and to

associate the subsets with each other;

a first control unit operable to control the second association unit so that processing thereof is repeatedly performed up to an uppermost layer;

a second control unit operable to control the first association unit, the second association unit, and the first control unit so that processings thereof are repeatedly performed on all subsets in the lowermost layer;

a first assignment unit operable to bring pieces of unique information into correspondence with the subsets in the lowermost layer respectively and to assign each piece of unique information to apparatus identifiers contained in the respective subset in the lowermost layer; and

a second assignment unit operable to bring pieces of derivative unique information into correspondence respectively with subsets each of which extends over two or more layers as a result of the associating and to assign each piece of derivative unique information to apparatus identifiers contained in the corresponding extending subset, the pieces of derivative unique information being derivatively obtained from the pieces of unique information.

26. The copyright protection system of Claim 25, wherein

the subset that is searched for by the first association unit and wholly contains said another subset in the lowermost layer is made up of a smallest number of elements, and the first association unit associates said another subset being a parent node with the searched subset being a child node,

the subset that is searched for by the second association unit

and wholly contains the containing subset being the association destination is made up of a smallest number of elements, and the second association unit associates the association destination subset being a parent node with the searched subset being a child node, and

the first control unit controls the second association unit so that processing thereof is performed repeatedly up to the uppermost layer and generates subset trees whose roots are the subsets in the lowermost layer.

27. The copyright protection system of Claim 26, wherein

the first association unit controls the second association unit so that processings thereof are repeatedly performed up to the uppermost layer, using one or more subsets obtained by excluding one or more subsets having been associated from subsets positioned in upper layers of the lowermost layer and generates subset trees whose roots are the subsets in the lowermost layer.

28. The copyright protection system of Claim 27, wherein

the second assignment unit generates the pieces of derivative unique information from the pieces of unique information, using a one-way function and brings the generated pieces of derivative unique information into correspondence with the extending subsets.

29. The copyright protection system of Claim 28, further comprising:

a unique information obtaining unit operable to obtain, in a case where a subset in which an identifier of a terminal apparatus

being a distribution destination of a piece of unique information appears as an element for a first time exists on one or more paths from the roots to one or more leaves of the subset trees, one or more pieces of unique information being in correspondence with such a subset; and

a distributing unit operable to distribute, to the terminal apparatus being the distribution destination, one or more groups each being made up of a different one of the obtained pieces of unique information and set identification information that identifies the subset that is in correspondence with the piece of unique information.

30. The copyright protection system of Claim 29, further comprising:

a first storing unit having an area for storing subsets being constituent elements of the subset trees and pieces of unique information that are respectively in correspondence with the subsets;

a second storing unit having an area for storing a plurality of nodes constituting the subset trees and child nodes of the plurality of nodes;

a first writing unit operable to write the subsets and the pieces of unique information into the first storing unit, while the subsets are brought into correspondence with the pieces unique information; and

a second writing unit operable to write the plurality of nodes and the child nodes of the plurality of nodes into the second storing unit, while the nodes are brought into correspondence with the child nodes.

31. The copyright protection system of Claim 30, wherein

the second control unit generates a plurality of subset trees by controlling the first association unit, the second association unit, and the first control unit so that the processings thereof are repeatedly performed on all the subsets in the lowermost layer,

the first storing unit stores therein subsets contained in the plurality of subset trees and pieces of unique information that are in correspondence with the contained subsets, and

the management apparatus further comprises:

a revoked identifier storing unit having an area for storing one or more revoked identifiers indicating one or more revoked terminal apparatuses out of the plurality of terminal apparatuses;

an encryption key generating unit operable to obtain one or more of the subsets from the first storing unit based on what is stored in the revoked identifier storing unit, to obtain one or more encryption keys based on pieces of unique information that are respectively in correspondence with the obtained subsets, to encrypt a media key used for utilization of a content with the obtained encryption keys individually, so as to generate encrypted media keys that are equal in number to the one or more encryption keys; and

a third writing unit operable to write, onto a recording medium mounted on the management apparatus, one or more groups each being made up of a different one of the encrypted media keys and a piece of reference identification information for identifying a subset used for obtaining the encryption key for the encrypted media key.

32. The copyright protection system of Claim 31, further

comprising:

a revoked identifier receiving unit operable to receive each revoked identifier and write the received revoked identifier into the revoked identifier storing unit.

33. The copyright protection system of Claim 31, wherein

the encryption keys are each a common key and are identical to the decryption keys,

the one-way function is further used for generating common keys based on the pieces of unique information from the pieces of unique information, and

the encryption key generating unit includes:

a subset obtaining unit operable to obtain, from the first storing unit, a subset that contains a largest number of one or more unrevoked identifiers which are other than the revoked identifiers stored in the revoked identifier storing unit;

a control unit operable to control the subset obtaining unit so that processing thereof is repeatedly performed until each of all the unrevoked identifiers belongs to any one of the one or more subsets obtained by the subset obtaining unit;

a common key obtaining unit operable to obtain, using the one-way function, one or more common keys generated from the pieces of unique information that are respectively in correspondence with the subsets obtained by the subset obtaining unit; and

an encrypting unit operable to generate encrypted media keys that are equal in number to the common keys, using the common keys obtained by the common key obtaining unit.

34. The copyright protection system of Claim 33, wherein the terminal apparatus comprises:

a unique information storing unit storing therein one or more groups each being made up of a piece of unique information distributed from the distributing unit of the management apparatus in advance and a piece of set identification information identifying a subset with which the piece of unique information is in correspondence;

a judging unit operable to judge whether the piece of set identification information indicates that the terminal apparatus is an unrevoked apparatus;

a first obtaining unit operable to, in a case where a judgment result of the judgment unit is in the affirmative, obtain one encrypted media key from the recording medium;

a second obtaining unit operable to obtain a decryption key that is in correspondence with the encryption key, using the piece of unique information stored in the unique information storing unit; and

a decrypting unit operable to decrypt the encrypted media key obtained by the first obtaining unit, using the decryption key obtained by the second obtaining unit, so as to generate the media key.

35. The copyright protection system of Claim 34, wherein the encryption key is a common key,

the judgment unit judges that the piece of set identification information indicates that the terminal apparatus is an unrevoked apparatus, in a case where a path exists that extends from the subset

being stored in the unique information storing unit and being identified by the piece of set identification information stored in the unique information storing unit and reaches the subset identified by the piece of reference identification information,

the first obtaining unit obtains an encrypted media key that is in correspondence with the piece of reference identification information,

the second obtaining unit obtains the decryption key and takes the obtained decryption key as the common key, and

the decrypting unit decrypts the encrypted media key, using the obtained common key.

36. The copyright protection system of Claim 35, wherein

the second obtaining unit includes:

a device key obtaining unit operable to generate and obtain a device key based on the piece of unique information and the piece of derivative unique information from the piece of unique information stored in the unique information storing unit, using a function identical to the one-way function;

a repetition unit operable to control the device key obtaining unit so that processing thereof is repeatedly performed using each piece of unique information obtained by the device key obtaining unit as a next input to the identical function, until a device key based on the piece of reference unique information is obtained; and

a decryption key obtaining unit operable to obtain, as the common key, the device key based on the piece of reference unique information obtained by the device key obtaining unit.

37. A recording medium including an encryption key storing unit that stores therein an encrypted media key which is obtained by encrypting a media key using an encryption key that (i) is in correspondence with a decryption key generated by an unrevoked terminal apparatus and (ii) is generated based on a piece of unique information that is in correspondence with a set being made up of one or more unrevoked terminal apparatuses.

38. The recording medium of Claim 37, wherein

the encryption key storing unit further stores therein a piece of set identification information for identifying a set that is in correspondence with the piece of unique information used in the generation of the encryption key.

39. A management apparatus that manages a plurality of terminal apparatuses by arranging apparatus identifiers for identifying the plurality of terminal apparatuses to be leaves of a tree structure and assigning pieces of unique information to the apparatus identifiers, the pieces of unique information being bases of decryption keys for decrypting a piece of encrypted data, the management apparatus comprising:

a subset generating unit operable to calculate and generate, for each of nodes in layers except for the leaves of the tree structure, a subset being made up of one or more apparatus identifiers positioned subordinate to the node;

a group generating unit operable to select, out of subsets positioned in a layer, and put into one group (i) a subset that contains

a smallest number of elements and (ii) another subset that contains the subset containing the smallest number of elements;

a first control unit operable to control the group generating unit so that processing thereof is repeatedly performed on all subsets each of which is positioned in the layer and contains the smallest number of elements;

a second control unit operable to control the group generating unit and the first control unit so that processings thereof are repeatedly performed on all of layers;

an integrating unit operable to, after the second control unit performs the processing on all of the layers, integrate into one group (i) a lower-layer group and (ii) an upper-layer group that includes a subset that wholly contains one of subsets belonging to the lower-layer group, the lower-layer group and the upper-layer group belonging to mutually different layers;

a first assignment unit operable to, after groups are integrated in all of the layers, bring pieces of unique information into correspondence with subsets each of which has a smallest number of elements in each of remaining groups and assign each piece of unique information to one or more apparatus identifiers contained in the corresponding subset; and

a second assignment unit operable to bring pieces of derivative unique information into correspondence with subsets other than the subset that has the smallest number of elements respectively and assigns each piece of derivative unique information to one or more apparatus identifiers that are contained in each of said other subsets, the pieces of derivative unique information being obtained derivatively from the pieces of unique information.

40. An association method to be used by a management apparatus that manages a plurality of terminal apparatuses by arranging apparatus identifiers for identifying the plurality of terminal apparatuses to be leaves of a tree structure and assigning pieces of unique information to the apparatus identifiers, the pieces of unique information being bases of decryption keys for decrypting a piece of encrypted data, the association method comprising:

a subset generating step of calculating and generating, for each of nodes in layers except for the leaves of the tree structure, a subset being made up of one or more apparatus identifiers positioned subordinate to the node;

a first association step of searching for a subset that wholly contains another subset positioned in a lowermost layer other than a leaf layer from an immediately upper layer, and associating the subsets with each other;

a second association step of searching for another subset that wholly contains the containing subset being an association destination from a same layer or an immediately upper layer and associating the subsets with each other;

a first control step of controlling the second association unit so that processing thereof is repeatedly performed up to an uppermost layer;

a second control step of controlling the first association unit, the second association unit, and the first control unit so that processings thereof are repeatedly performed on all subsets in the lowermost layer;

a first assignment step of bringing pieces of unique information

into correspondence with the subsets in the lowermost layer respectively and assigning each piece of unique information to apparatus identifiers contained in the corresponding subset in the lowermost layer; and

a second assignment step of bringing pieces of derivative unique information into correspondence respectively with subsets each of which extends over two or more layers as a result of the associating and assigning each piece of derivative unique information to apparatus identifiers contained in the corresponding extending subset, the pieces of derivative unique information being derivatively obtained from the pieces of unique information.

41. A program that is for making associations and that has a management apparatus execute the following steps, the management apparatus managing a plurality of a plurality of terminal apparatuses by arranging apparatus identifiers for identifying the plurality of terminal apparatuses to be leaves of a tree structure and assigning pieces of unique information to the apparatus identifiers, the pieces of unique information being bases of decryption keys for decrypting a piece of encrypted data, the steps being:

a subset generating step of calculating and generating, for each of nodes in layers except for the leaves of the tree structure, a subset being made up of one or more apparatus identifiers positioned subordinate to the node;

a first association step of searching for a subset that wholly contains another subset positioned in a lowermost layer other than a leaf layer from an immediately upper layer, and associating the subsets with each other;

a second association step of searching for another subset that wholly contains the containing subset being an association destination from a same layer or an immediately upper layer and associating the subsets with each other;

a first control step of controlling the second association unit so that processing thereof is repeatedly performed up to an uppermost layer;

a second control step of controlling the first association unit, the second association unit, and the first control unit so that processings thereof are repeatedly performed on all subsets in the lowermost layer;

a first assignment step of bringing pieces of unique information into correspondence with the subsets in the lowermost layer respectively and assigning each piece of unique information to apparatus identifiers contained in the corresponding subset in the lowermost layer; and

a second assignment step of bringing pieces of derivative unique information into correspondence respectively with subsets each of which extends over two or more layers as a result of the associating and assigning each piece of derivative unique information to apparatus identifiers contained in the corresponding extending subset, the pieces of derivative unique information being derivatively obtained from the pieces of unique information.

42. A computer-readable program recording medium which records thereon a program that is for making associations and has a management apparatus execute the following steps, the management apparatus managing a plurality of a plurality of terminal apparatuses by

arranging apparatus identifiers for identifying the plurality of terminal apparatuses to be leaves of a tree structure and assigning pieces of unique information to the apparatus identifiers, the pieces of unique information being bases of decryption keys for decrypting a piece of encrypted data, the steps being:

a subset generating step of calculating and generating, for each of nodes in layers except for the leaves of the tree structure, a subset being made up of one or more apparatus identifiers positioned subordinate to the node;

a first association step of searching for a subset that wholly contains another subset positioned in a lowermost layer other than a leaf layer from an immediately upper layer, and associating the subsets with each other;

a second association step of searching for another subset that wholly contains the containing subset being an association destination from a same layer or an immediately upper layer and associating the subsets with each other;

a first control step of controlling the second association unit so that processing thereof is repeatedly performed up to an uppermost layer;

a second control step of controlling the first association unit, the second association unit, and the first control unit so that processings thereof are repeatedly performed on all subsets in the lowermost layer;

a first assignment step of bringing pieces of unique information into correspondence with the subsets in the lowermost layer respectively and assigning each piece of unique information apparatus identifiers contained in the corresponding subset in the lowermost

layer; and

a second assignment step of bringing pieces of derivative unique information into correspondence respectively with subsets each of which extends over two or more layers as a result of the associating and assigning each piece of derivative unique information to apparatus identifiers contained in the corresponding extending subset, the pieces of derivative unique information being derivatively obtained from the pieces of unique information.